CLAIMS

1. A method for combating spam comprising:

classifying a message at least partially by evaluating at least one message parameter, using at least one variable criterion, thereby providing a spam classification; and

handling said message based on said spam classification.

2. A method for combating spam according to claim 1 and wherein said at least one variable criterion comprises a criterion which changes over time.

3. A method for combating spam according to claim 1 or claim 2 and wherein said at least one variable criterion comprises a parameter template-defined function.

4. A method for combating spam according to any of claims 1 - 3 and wherein said classifying comprises:

said using at least one variable criterion at at least one gateway; and

said providing spam classifications at at least one server, receiving evaluation outputs from said at least one gateway and providing said spam classifications to said at least one gateway.

5. A method for combating spam according to claim 4 and wherein said classifying also comprises:

encrypting at least part of said evaluation outputs by employing a non-reversible encryption so as to generate encrypted information; and

transmitting at least said encrypted information to said at least one server.

6. A method for combating spam according to claim 5 and wherein said transmitting comprises transmitting information of a length limited to a predefined threshold.

7. A method for combating spam according to any of claims 1 - 6 and wherein said handling comprises at least one of:

forwarding said message to an addressee of said message;

storing said message in a predefined storage area;

deleting said message;

rejecting said message;

sending said message to an originator of said message; and

delaying said message for a period of time and thereafter re-classifying said message.

8. A method for combating spam according to any of claims 1 - 7 and wherein said message comprises at least one of:

an e-mail;

a network packet;

a digital telecom message; and

an instant messaging message.

9. A method for combating spam according to any of claims 1 - 8 and wherein said classifying also comprises at least one of:

requesting feedback from an addressee of said message;

evaluating compliance of said message with a predefined policy;

evaluating registration status of at least one registered address in said message;

analyzing a match among network references in said message;

analyzing a match between at least one translatable address in said message and at least one other network reference in said message;

at least partially actuating an unsubscribe feature in said message;

analyzing an unsubscribe feature in said message;

employing a variable criteria;

sending information to a server and receiving classification data based on said information;

employing classification data received from a server; and

employing stored classification data.

10. A method for combating spam comprising:

classifying messages at least partially by evaluating at least one message parameter of multiple messages, by employing at least one evaluation criterion which changes over time, thereby providing spam classifications; and

handling said messages based on said spam classifications.

11. A method for combating spam according to claim 10 and wherein said classifying is at least partially responsive to similarities between plural messages among said multiple messages, which similarities are reflected in said at least one message parameter.

12. A method for combating spam according to claim 10 or claim 11 and wherein said classifying is at least partially responsive to similarities between plural messages among said multiple messages, which similarities are reflected in outputs of applying said at least one evaluation criterion to said at least one message parameter.

13. A method for combating spam according to any of claims 10 - 12 and wherein said classifying is at least partially responsive to similarities in multiple outputs of applying a single evaluation criterion to said at least one message parameter in multiple messages.

14. A method for combating spam according to any of claims 10 - 13 and wherein said classifying is at least partially responsive to the extent of similarities between plural messages among said multiple messages which similarities are reflected in said at least one message parameter.

15. A method for combating spam according to any of claims 10 - 14 and wherein said classifying is at least partially responsive to the extent of similarities between plural messages among said multiple messages which similarities are reflected

in outputs of applying said at least one evaluation criterion to said at least one message parameter.

16. A method for combating spam according to any of claims 10 - 15 and wherein said classifying is at least partially responsive to the extent of similarities in multiple outputs of applying a single evaluation criterion to said at least one message parameter in multiple messages.

17. A method for combating spam according to any of claims 14 - 16 and wherein said extent of similarities comprises a count of messages among said multiple messages which are similar.

18. A method for combating spam according to any of claims 10 - 17 and wherein said classifying is at least partially responsive to similarities in outputs of applying evaluation criteria to said at least one message parameter in multiple messages, wherein a plurality of different evaluation criteria are individually applied to said at least one message parameter in said multiple messages, yielding a corresponding plurality of outputs indicating a corresponding plurality of similarities among said multiple messages.

19. A method according to claim 18 and wherein said classifying also comprises aggregating individual similarities among said plurality of similarities.

20. A method according to claim 19 and wherein said aggregating individual similarities among said plurality of similarities comprises applying weights to said individual similarities.

21. A method according to claim 19 and wherein said aggregating individual similarities among said plurality of similarities comprises calculating a polynomial over said individual similarities.

22. A method for combating spam according to any of claims 10 - 21 and wherein said classifying is at least partially responsive to extents of similarities in outputs of applying evaluation criteria to said at least one message parameter in multiple messages, wherein a plurality of different evaluation criteria are individually applied to said at least one message parameter in said multiple messages, yielding a corresponding plurality of outputs indicating a corresponding plurality of extents of similarities among said multiple messages.

23. A method according to claim 22 and wherein said classifying also comprises aggregating individual extents of similarities among said plurality of extents of similarities.

24. A method according to claim 23 and wherein said aggregating individual extents of similarities among said plurality of extents of similarities comprises applying weights to said individual extents similarities.

25. A method according to claim 23 and wherein said aggregating individual extents of similarities among said plurality of extents of similarities comprises calculating a polynomial over said individual extents of similarities.

26. A method for combating spam according to any of claims 22 - 25 and wherein said extents of similarities comprises a count of messages among said multiple messages which are similar.

27. A method for combating spam according to any of claims 10 - 26 and wherein said at least one evaluation criterion comprises a parameter template-defined function.

28. A method for combating spam according to any of claims 10 - 27 and wherein said classifying employs a function of outputs of evaluating at least one message parameter of said multiple messages

29. A method for combating spam according to claim 28 and wherein said classifying is at least partially responsive to similarities between outputs of said evaluating at least one message parameter of multiple messages.

30. A method for combating spam according to any of claims 10 - 29 and wherein said classifying comprises:

said evaluating at at least one gateway; and

said providing spam classifications at at least one server, receiving evaluation outputs from said at least one gateway and providing said spam classifications to said at least one gateway.

31. A method for combating spam according to claim 30 and wherein said classifying also comprises:

encrypting at least part of said evaluation outputs by employing a non-reversible encryption so as to generate encrypted information; and

transmitting at least said encrypted information to said at least one server.

32. A method for combating spam according to claim 31 and wherein said transmitting comprises transmitting information of a length limited to a predefined threshold.

33. A method for combating spam according to any of claims 10 - 32 and wherein said handling comprises at least one of:

forwarding said messages to addressees of said messages;

storing said messages in a predefined storage area;

deleting said messages;

rejecting said messages;

sending said messages to originators of said messages; and

delaying said messages for a period of time and thereafter re-classifying said messages.

34. A method for combating spam according to any of claims 10 - 33 and wherein said messages comprise at least on of:

an e-mail;

network packets;

digital telecom messages; and

instant messaging messages.

35. A method for combating spam according to any of claims 10 - 34 and wherein said classifying also comprises at least one of:

requesting feedback from an addressee of said messages;

evaluating compliance of said messages with a predefined policy;

evaluating registration status of at least one registered address in said messages;

analyzing a match among network references in said messages

analyzing a match between at least one translatable address in said messages and at least one other network reference in said messages;

at least partially actuating an unsubscribe feature in said messages;

analyzing an unsubscribe feature in said messages;

employing a variable criteria;

sending information to a server and receiving classification data based thereon;

employing classification data received from a server; and

employing stored classification data.

36. A method for combating spam comprising:

categorizing incoming messages received at at least one gateway into at least first, second and third categories;

providing spam classifications for incoming messages in at least said first and second categories;

not immediately providing a spam classification for incoming messages in said third category;

storing incoming messages in said third category; and

thereafter providing spam classifications for said incoming messages in said third category.

37. A method for combating spam according to claim 36 and also comprising:

handling said incoming messages based on said spam classifications.

38. A method for combating spam according to claim 37 and wherein said handling comprises one or more of:

forwarding said messages to addressees of said messages;

storing said messages in a predefined storage area;

deleting said messages;

rejecting said messages;

sending said messages to originators of said messages; and

delaying said messages for a period of time and thereafter re-classifying said messages.

39. A method for combating spam according to any of claims 36 - 38 and wherein said providing a spam classification for said incoming messages in said third category also comprises providing a spam classification for a second message received at said at least one gateway.

40. A method for combating spam according to any of claims 36 - 39 and also comprising waiting up to a predetermined period of time between said providing spam classifications for incoming messages in at least said first and second categories and said thereafter providing a spam classification for said incoming messages in said third category.

41. A method for combating spam according to any of claims 36 - 40 and wherein said incoming messages comprise at least one of:

e-mail messages;

network packets;

digital telecom messages; and

instant messaging messages.

42. A method for combating spam according to any of claims 36 – 41 and wherein said categorizing comprises at least one of:

requesting feedback from an addressee of said messages;

evaluating compliance of said messages with a predefined policy;

evaluating registration status of at least one registered address in said messages;

analyzing a match among network references in said messages

analyzing a match between at least one translatable address in said messages and at least one other network reference in said messages;

at least partially actuating an unsubscribe feature in said messages;

analyzing an unsubscribe feature in said messages;

employing a variable criteria;

sending information to a server and receiving categorization data based thereon;

employing categorization data received from a server; and

employing stored categorization data.

43. A method for combating spam according to any of claims 36 – 41 and wherein said providing spam classifications comprises at least one of:

requesting feedback from an addressee of said messages;

evaluating compliance of said messages with a predefined policy;

evaluating registration status of at least one registered address in said messages;

analyzing a match among network references in said messages

analyzing a match between at least one translatable address in said messages and at least one other network reference in said messages;

at least partially actuating an unsubscribe feature in said messages;

analyzing an unsubscribe feature in said messages;

employing a variable criteria;

sending information to a server and receiving classification data based thereon;

employing classification data received from a server; and

employing stored classification data.

44. A method for combating spam comprising:

classifying a message at least partially by relating to an unsubscribe feature in the message, thereby providing spam classifications for said message; and

handling said message based on said spam classifications.

45. A method for combating spam according to claim 44 and wherein said classifying also comprises identifying whether said message includes an unsubscribe feature.

46. A method for combating spam according to claim 44 or claim 45 and wherein said classifying also comprises identifying whether said unsubscribe feature includes a reference to an addressee of said message.

47. A method for combating spam according to claim 46 and wherein said reference to an addressee of said message comprises an e-mail address.

48. A method for combating spam according to claim 46 and wherein said reference to an addressee of said message comprises a per-addressee generated ID.

49. A method for combating spam according to claim 48 and wherein said per-addressee generated ID comprises a user identification number.

50. A method for combating spam comprising:

classifying a message at least partially by at least partially actuating an unsubscribe feature in the message, thereby providing spam classifications for said messages; and

handling said message based on said spam classifications.

51. A method for combating spam according to claim 50 and wherein said classifying comprises analyzing an output of said at least partial actuation.

52. A method for combating spam according to claim 51 and wherein said analyzing an output of said at least partially actuating comprising sensing whether part of said output indicates the occurrence of an error.

53. A method for combating spam according to claim 52 and wherein said at least partially actuating also comprises at least attempting communication with a network server.

54. A method for combating spam according to claim 53 and wherein said error indicates that said network server does not exist.

55. A method for combating spam according to claim 53 and wherein said error indicates that said network server does not provide an unsubscribe functionality.

56. A method for combating spam according to claim 53 and wherein said error indicates that said network server cannot unsubscribe a message addressee.

57. A method for combating spam according to claim 51 and wherein said analyzing an output of said at least partially actuating comprises sensing whether part of said output comprises an addressee reference.

58. A method for combating spam according to claim 57 and wherein said addressee reference comprises an e-mail address.

59. A method for combating spam according to claim 57 and wherein said addressee reference comprises a per-addressee generated ID.

60. A method for combating spam according to claim 59 and wherein said per-addressee generated ID comprises a user identification number.

61. A method for combating spam according to any of claims 57 - 60 and wherein said analyzing an output of said at least partially actuating also comprises relating said addressee reference to at least one addressee reference characteristic of said message.

62. A method for combating spam according to claim 61 and wherein said at least one addressee reference characteristic of said message comprises an e-mail address.

63. A method for combating spam according to claim 61 and wherein said at least one addressee reference characteristic of said message comprises a per-addressee generated ID.

64. A method for combating spam according to claim 63 and wherein said per- at least one addressee reference characteristic of said per-addressee generated ID comprises a user identification number.

65. A method for combating spam according to any of claims 44 – 64 and wherein said classifying also comprises recognizing said unsubscribe feature.

66. A method for combating spam according to claim 65 and wherein said recognizing said unsubscribe feature comprises sensing a part of said message comprising predefined keywords.

67. A method for combating spam according to claim 65 and wherein said recognizing said unsubscribe feature comprises sensing a part of said message comprising a network reference and a reference to an addressee of said messages.

68. A method for combating spam according to claim 67 and wherein said network reference comprises a reference to a network server.

69. A method for combating spam according to claim 67 or claim 68 and wherein said reference to an addressee of said message comprises an addressee e-mail address.

70. A method for combating spam according to any of claims 44 – 69 and wherein said handling comprises one or more of:

forwarding said message to an addressee of said message;

storing said message in a predefined storage area;

deleting said message;

rejecting said message;

sending said message to an originator of said message; and

delaying said message for a period of time and thereafter re-classifying said message.

71. A method for combating spam according to any of claims 44 –70 and wherein said message comprises at least one of:

an e-mail;

a network packet;

a digital telecom message; and

an instant messaging message.

72. A method for combating spam according to any of claims 44 –71 and wherein said classifying also comprises at least one of:

requesting feedback from an addressee of said message;

evaluating compliance of said message with a predefined policy;

evaluating registration status of at least one registered address in said message;

analyzing a match among network references in said message;

analyzing a match between at least one translatable address in said message and at least one other network reference in said message;

at least partially actuating an unsubscribe feature in said message;

analyzing an unsubscribe feature in said message;

employing a variable criteria;

sending information to a server and receiving classification data based thereon;

employing classification data received from a server; and

employing stored classification data.

73. A method for combating spam comprising:

classifying a message at least partially by relating to registration status of at least one registered address in said message, thereby providing a spam classification for said message; and

handling said message based on said spam classifications.

74. A method for combating spam according to claim 73 and wherein said classifying comprises employing a network service for determining said registration status.

75. A method for combating spam according to claim 73 or claim 74 and wherein said registration status comprises a registration date.

76. A method for combating spam according to claim 73 or claim 74 and wherein said registration status comprises a registration expiry date.

77. A method for combating spam according to any of claims 73 - 76 and wherein said classifying comprises inspecting whether registration of said registered address has expired.

78. A method for combating spam according to any of claims 73 - 76 and wherein said classifying comprises inspecting whether said registered address has not been registered.

79. A method for combating spam according to claim 75 and wherein said classifying comprises comparing said registration date to a predefined date.

80. A method for combating spam according claim 79 and wherein said predefined date is a current date.

81. A method for combating spam according to any of claims 73 – 80 and wherein said registered address comprises an internet domain name.

82. A method for combating spam according claim 81 and wherein said internet domain name is parked.

83. A method for combating spam according to any of claims 73 – 82 and wherein said handling comprises at least one of:

forwarding said message to an addressee of said message;

storing said message in a predefined storage area;

deleting said message;

rejecting said message;

sending said message to an originator of said message; and

delaying said message for a period of time and thereafter re-classifying said message.

84. A method for combating spam according to any of claims 73 – 83 and wherein said message comprises at least one of:

an e-mail;

a network packet;

a digital telecom message; and

an instant messaging message.

85. A method for combating spam according to any of claims 73 – 84 and wherein said classifying also comprises at least one of:

requesting feedback from an addressee of said message;

evaluating compliance of said message with a predefined policy;

evaluating registration status of at least one registered address in said message;

analyzing a match among network references in said message;

analyzing a match between at least one translatable address in said message and at least one other network reference in said message;

at least partially actuating an unsubscribe feature in said message;

analyzing an unsubscribe feature in said message;

employing a variable criteria;

sending information to a server and receiving classification data based thereon;

employing classification data received from a server; and

employing stored classification data.

86. A method for combating spam comprising:

classifying a message at least partially by relating to a match among network references in said message, thereby providing a spam classification for said message; and

handling said message based on said spam classification.

87. A method for combating spam according to claim 86 and wherein said network references include at least one translatable network address and wherein said match is between at least one translatable network address and another at least one of said network references.

88. A method for combating spam according to claim 87 and wherein said at least one translatable network address comprises a registered network address.

89. A method for combating spam according to claim 87 and wherein said at least one translatable network address comprises an internet domain name.

90. A method for combating spam according to any of claims 87 – 89 and wherein said classifying also comprises translating said translatable network address, thereby providing a translated network address.

91. A method for combating spam according to any of claims 86 – 90 and wherein said handling comprises at least one of:

forwarding said message to an addressee of said message;

storing said message in a predefined storage area;

deleting said message;

rejecting said message;

sending said message to an originator of said message; and

delaying said message for a period of time and thereafter re-classifying said message.

92. A method for combating spam according to any of claims 86 – 91 and wherein said message comprises at least one of:

an e-mail;

a network packet;

a digital telecom message; and

an instant messaging message.

93. A method for combating spam according to any of claims 86 – 92 and wherein said classifying also comprises at least one of:

requesting feedback from an addressee of said message;

evaluating compliance of said message with a predefined policy;

evaluating registration status of at least one registered address in said message;

analyzing a match among network references in said message;

analyzing a match between at least one translatable address in said message and at least one other network reference in said message;

at least partially actuating an unsubscribe feature in said message;

analyzing an unsubscribe feature in said message;

employing a variable criteria;

sending information to a server and receiving classification data based thereon;

employing classification data received from a server; and

employing stored classification data.

94. A system for combating spam comprising:

a message evaluator, operative to evaluate a message using at least one message parameter, said at least one message parameter comprising at least one variable criterion;

a message classifier, operative to provide a spam classification of said message at least partially based on an output of said message evaluator; and

a message handler, operative to handle said message based on said spam classification.

95. A system for combating spam according to claim 94 and wherein said at least one variable criterion comprises a criterion which changes over time.

96. A system for combating spam according to claim 94 or claim 95 and wherein said at least one variable criterion comprises a parameter template-defined function.

97. A system for combating spam according to any of claims 94 - 96 and wherein:

said message evaluator includes at least one gateway; and

said message classifier includes at least one server; and

said at least one server is operative to receive said output from said at least one gateway and to provide said spam classification to said at least one gateway.

98. A system for combating spam according to claim 97 and wherein said at least one gateway also comprises:

an encrypter, operative to encrypt at least part of said output by employing a non-reversible encryption so as to generate encrypted information; and

a transmitter, operative to transmit at least said encrypted information to said at least one server.

99. A system for combating spam according to claim 98 and wherein said transmitter is operative to transmit information of a length limited to a predefined threshold.

100. A system for combating spam according to any of claims 94 - 99 and wherein said message handler is operative to perform at least one of the following:

forward said message to an addressee of said message;

store said message in a predefined storage area;

delete said message;

reject said message;

send said message to an originator of said message; and

delay said message for a period of time and thereafter re-classify said message.

101. A system for combating spam according to any of claims 94 - 100 and wherein said message comprises at least one of:

an e-mail;

a network packet;

a digital telecom message; and

an instant messaging message.

102. A system for combating spam according to any of claims 94 - 101 and wherein said message classifier is operative to provide said spam classification at least partially based on at least one of the following:

feedback requested from an addressee of said message;

compliance of said message with a predefined policy;

a registration status of at least one registered address in said message;

a match among network references in said message;

a match between at least one translatable address in said message and at least one other network reference in said message;

at least partial actuation of an unsubscribe feature in said message;

an analysis of an unsubscribe feature in said message;

a variable criteria;

information sent to a server and classification data received based on said information;

classification data received from a server; and

stored classification data.

103. A system for combating spam comprising:

a message evaluator, operative to evaluate multiple messages using at least one message parameter of said multiple messages, said at least one message parameter comprising at least one variable criterion which changes over time;

a message classifier, operative to provide spam classifications of said messages at least partially based on outputs of said message evaluator; and

a message handler, operative to handle said messages based on said spam classifications.

104. A system for combating spam according to claim 103 and wherein said spam classifications are at least partially based on similarities between plural messages among said multiple messages, which similarities are reflected in said at least one message parameter.

105. A system for combating spam according to claim 103 or claim 104 and wherein said spam classifications are at least partially based on similarities between plural messages among said multiple messages, which similarities are reflected in

outputs of applying said at least one evaluation criterion to said at least one message parameter.

106. A system for combating spam according to any of claims 103 - 105 and wherein said spam classifications are at least partially based on similarities in multiple outputs of applying a single evaluation criterion to said at least one message parameter in multiple messages.

107. A system for combating spam according to any of claims 103 - 106 and wherein said spam classifications are at least partially based on the extent of similarities between plural messages among said multiple messages which similarities are reflected in said at least one message parameter.

108. A system for combating spam according to any of claims 103 - 107 and wherein said spam classifications are at least partially based on the extent of similarities between plural messages among said multiple messages which similarities are reflected in outputs of applying said at least one evaluation criterion to said at least one message parameter.

109. A system for combating spam according to any of claims 103 - 108 and wherein said spam classifications are at least partially based on the extent of similarities in multiple outputs of applying a single evaluation criterion to said at least one message parameter in multiple messages.

110. A system for combating spam according to any of claims 107 - 109 and wherein said extent of similarities comprises a count of messages among said multiple messages which are similar.

111. A system for combating spam according to any of claims 103 - 110 and wherein said spam classifications are at least partially based on similarities in outputs of applying evaluation criteria to said at least one message parameter in multiple messages, wherein a plurality of different evaluation criteria are individually applied to said at

least one message parameter in said multiple messages, yielding a corresponding plurality of outputs indicating a corresponding plurality of similarities among said multiple messages.

112. A system according to claim 111 and wherein said message classifier also comprises an aggregator, operative to aggregate individual similarities among said plurality of similarities.

113. A system according to claim 112 and wherein said aggregator is operative to apply a weighting to said individual similarities.

114. A system according to claim 112 and wherein said aggregator is operative to calculate a polynomial over said individual similarities.

115. A system for combating spam according to any of claims 103 - 114 and wherein said spam classifications are at least partially based on extents of similarities in outputs of applying evaluation criteria to said at least one message parameter in multiple messages, wherein a plurality of different evaluation criteria are individually applied to said at least one message parameter in said multiple messages, yielding a corresponding plurality of outputs indicating a corresponding plurality of extents of similarities among said multiple messages.

116. A system according to claim 115 and wherein said message classifier also comprises an aggregator, operative to aggregate individual extents of similarities among said plurality of extents of similarities.

117. A system according to claim 116 and wherein said aggregator is operative to apply a weighting to said individual extents similarities.

118. A system according to claim 116 and wherein said aggregator is operative to calculate a polynomial over said individual extents of similarities.

119. A system for combating spam according to any of claims 115 - 118 and wherein said extents of similarities comprise a count of messages among said multiple messages which are similar.

120. A system for combating spam according to any of claims 103 - 119 and wherein said at least one variable criterion comprises a parameter template-defined function.

121. A system for combating spam according to any of claims 103 - 120 and wherein said message classifier is operative to employ a function of outputs of evaluating at least one message parameter of said multiple messages.

122. A system for combating spam according to claim 121 and wherein said spam classifications are at least partially based on similarities between outputs of said evaluating at least one message parameter of multiple messages.

123. A system for combating spam according to any of claims 103 - 122 and wherein:

said message evaluator includes at least one gateway;

said message classifier includes at least one server; and

said at least one server is operative to receive said outputs from said at least one gateway and to provide said spam classifications to said at least one gateway.

124. A system for combating spam according to claim 123 and wherein said at least one gateway also comprises:

an encrypter, operative to encrypt at least part of said outputs by employing a non-reversible encryption so as to generate encrypted information; and

a transmitter, operative to transmit at least said encrypted information to said at least one server.

125. A system for combating spam according to claim 124 and wherein said transmitter is operative to transmit information of a length limited to a predefined threshold.

126. A system for combating spam according to any of claims 103 - 125 and wherein said message handler is operative to perform at least one of the following:

forward at least one of said messages to an addressee of said at least one of said messages;

store at least one of said messages in a predefined storage area;

delete at least one of said messages;

reject at least one of said messages;

send at least one of said messages to an originator of said at least one of said messages; and

delay at least one of said messages for a period of time and thereafter re-classify said at least one of said messages.

127. A system for combating spam according to any of claims 103 - 126 and wherein said messages comprise at least one of:

e-mail messages;

network packets;

digital telecom messages; and

instant messaging messages.

128. A system for combating spam according to any of claims 103 - 127 and wherein said message classifier is operative to provide said spam classification at least partially based on at least one of the following:

feedback requested from addressees of said messages;

compliance of said messages with a predefined policy;

a registration status of at least one registered address in said messages;

a match among network references in said messages;

a match between at least one translatable address in said messages and at least one other network reference in said messages;

at least partial actuation of an unsubscribe feature in said messages;

an analysis of an unsubscribe feature in said messages;

a variable criteria;

information sent to a server and classification data received based on said information;

classification data received from a server; and

stored classification data.

129. A system for combating spam comprising:

a message categorizer, operative to categorize incoming messages received at at least one gateway into at least first, second and third categories; and

a message classifier, operative to provide spam classifications for incoming messages in at least said first and second categories, said message classifier being operative to store incoming messages in said third category and at a time thereafter to provide spam classifications for said incoming messages in said third category.

130. A system for combating spam according to claim 129 and also comprising a message handler, operative to handle said incoming messages based on said spam classifications.

131. A system for combating spam according to claim 130 and wherein said message handler is operative to perform at least one of the following:

forward at least one of said messages to an addressee of said at least one of said messages;

store at least one of said messages in a predefined storage area;

delete at least one of said messages;

reject at least one of said messages;

send at least one of said messages to an originator of said at least one of said messages; and

delay at least one of said messages for a period of time and thereafter re-classify said at least one of said messages.

132. A system for combating spam according to any of claims 129 - 131 and wherein said message classifier is operative to provide a spam classification for a second message received at said at least one gateway at said time thereafter.

133. A system for combating spam according to any of claims 129 - 132 and wherein said time thereafter comprises a time not later than after a maximum predetermined waiting period.

134. A system for combating spam according to any of claims 129 - 133 and wherein said incoming messages comprise at least one of:

e-mail messages;

network packets;

digital telecom messages; and

instant messaging messages.

135. A system for combating spam according to any of claims 129 – 135 and wherein said message categorizer is operative to categorize said messages at least partially based on at least one of the following:

feedback requested from addressees of said messages;

compliance of said messages with a predefined policy;

a registration status of at least one registered address in said messages;

a match among network references in said messages;

a match between at least one translatable address in said messages and at least one other network reference in said messages;

at least partial actuation of an unsubscribe feature in said messages;

an analysis of an unsubscribe feature in said messages;

a variable criteria;

information sent to a server and classification data received based on said information;

categorization data received from a server; and

stored categorization data.

136. A system for combating spam according to any of claims 129 – 135 and wherein said message classifier is operative to provide said spam classification at least partially based on at least one of the following:

feedback requested from addressees of said messages;

compliance of said messages with a predefined policy;

a registration status of at least one registered address in said messages;

a match among network references in said messages;

a match between at least one translatable address in said messages and at least one other network reference in said messages;

at least partial actuation of an unsubscribe feature in said messages;

an analysis of an unsubscribe feature in said messages;

a variable criteria;

information sent to a server and classification data received based on said information;

classification data received from a server; and

stored classification data.

137. A system for combating spam comprising:

a message classifier, operative to provide a spam classification for a message at least partially by relating to an unsubscribe feature in said message; and

a message handler, operative to handle said message based on said spam classification.

138. A system for combating spam according to claim 137 and also comprising an unsubscribe identifier, operative to identify whether said message includes an unsubscribe feature.

139. A system for combating spam according to claim 137 or claim 138 and also comprising an addressee identifier, operative to identify whether said unsubscribe feature includes a reference to an addressee of said message.

140. A system for combating spam according to claim 139 and wherein said reference to an addressee of said message comprises an e-mail address.

141. A system for combating spam according to claim 139 and wherein said reference to an addressee of said message comprises a per-addressee generated ID.

142. A system for combating spam according to claim 141 and wherein said per-addressee generated ID comprises a user identification number.

143. A system for combating spam comprising:

a message classifier, operative to provide a spam classification for a message at least partially by at least partial actuation of an unsubscribe feature in the message; and

a message handler, operative to handle said message based on said spam classification.

144. A system for combating spam according to claim 143 and also comprising an actuation analyzer operative to analyze an output of said at least partial actuation.

145. A system for combating spam according to claim 144 and wherein said analyzer is operative to sense whether part of said output indicates the occurrence of an error.

146. A system for combating spam according to claim 145 and wherein said at least partial actuation also comprises at least attempting communication with a network server.

147. A system for combating spam according to claim 146 and wherein said error indicates that said network server does not exist.

148. A system for combating spam according to claim 146 and wherein said error indicates that said network server does not provide an unsubscribe functionality.

149. A system for combating spam according to claim 146 and wherein said error indicates that said network server cannot unsubscribe a message addressee.

150. A system for combating spam according to claim 144 and wherein said analyzer is operative to sense whether part of said output comprises an addressee reference.

151. A system for combating spam according to claim 150 and wherein said addressee reference comprises an e-mail address.

152. A system for combating spam according to claim 150 and wherein said addressee reference comprises a per-addressee generated ID.

153. A system for combating spam according to claim 152 and wherein said per-addressee generated ID comprises a user identification number.

154. A system for combating spam according to any of claims 150 - 153 and wherein said analyzer is operative to relate said addressee reference to at least one addressee reference characteristic of said message.

155. A system for combating spam according to claim 154 and wherein said at least one addressee reference characteristic of said message comprises an e-mail address.

156. A system for combating spam according to claim 154 and wherein said at least one addressee reference characteristic of said message comprises a per-addressee generated ID.

157. A system for combating spam according to claim 156 and wherein said per- at least one addressee reference characteristic of said per-addressee generated ID comprises a user identification number.

158. A system for combating spam according to any of claims 137 – 157 and also comprising an unsubscribe recognizer, operative to recognize said unsubscribe feature.

159. A system for combating spam according to claim 158 and wherein said unsubscribe recognizer is operative to sense a part of said message comprising predefined keywords.

160. A system for combating spam according to claim 159 and wherein said unsubscribe recognizer is operative to sense a part of said message comprising a network reference and a reference to an addressee of said messages.

161. A system for combating spam according to claim 160 and wherein said network reference comprises a reference to a network server.

162. A system for combating spam according to claim 160 or claim 161 and wherein said reference to an addressee of said message comprises an addressee e-mail address.

163. A system for combating spam according to any of claims 137 – 162 and wherein said message handler is operative to perform at least one of the following:

forward said message to an addressee of said message;

store said message in a predefined storage area;

delete said message;

reject said message;

send said message to an originator of said message; and

delay said message for a period of time and thereafter re-classify said message.

164. A system for combating spam according to any of claims 137 – 163 and wherein said message comprises at least one of:

an e-mail;

a network packet;

a digital telecom message; and

an instant messaging message.

165. A system for combating spam according to any of claims 137 – 164 and wherein said message classifier is operative to provide said spam classification at least partially based on at least one of the following:

feedback requested from an addressee of said message;

compliance of said message with a predefined policy;

a registration status of at least one registered address in said message;

a match among network references in said message;

a match between at least one translatable address in said message and at least one other network reference in said message;

at least partial actuation an unsubscribe feature in said message;

an analysis of an unsubscribe feature in said message;

a variable criteria;

information sent to a server and classification data received based on said information;

classification data received from a server; and

stored classification data.

166. A system for combating spam comprising:

a message classifier, operative to provide a spam classification for a message at least partially by relating to registration status of at least one registered address in said message; and

a message handler, operative to handle said message based on said spam classifications.

167. A system for combating spam according to claim 166 and wherein said message classifier is operative to employ a network service for determining said registration status.

168. A system for combating spam according to claim 166 or claim 167 and wherein said registration status comprises a registration date.

169. A system for combating spam according to claim 166 or claim 167 and wherein said registration status comprises a registration expiry date.

170. A system for combating spam according to any of claims 166 - 169 and wherein said message classifier is operative to inspect whether registration of said registered address has expired.

171. A system for combating spam according to any of claims 166 - 169 and wherein said message classifier is operative to inspect whether said registered address has not been registered.

172. A system for combating spam according to claim 168 and wherein said message classifier is operative to compare said registration date to a predefined date.

173. A system for combating spam according claim 172 and wherein said predefined date is a current date.

174. A system for combating spam according to any of claims 166 – 173 and wherein said registered address comprises an Internet domain name.

175. A system for combating spam according claim 174 and wherein said Internet domain name is parked.

176. A system for combating spam according to any of claims 166 – 175 and wherein said message handler is operative to perform at least one of the following:

forward said message to an addressee of said message;

store said message in a predefined storage area;

delete said message;

reject said message;

send said message to an originator of said message; and

delay said message for a period of time and thereafter re-classify said message.

177. A system for combating spam according to any of claims 166 – 176 and wherein said message comprises at least one of:

an e-mail;

a network packet;

a digital telecom message; and

an instant messaging message.

178. A system for combating spam according to any of claims 166 – 177 and wherein said message classifier is operative to provide said spam classification at least partially based on at least one of the following:

feedback requested from an addressee of said message;

compliance of said message with a predefined policy;

a registration status of at least one registered address in said message;

a match among network references in said message;

a match between at least one translatable address in said message and at least one other network reference in said message;

at least partial actuation an unsubscribe feature in said message;

an analysis of an unsubscribe feature in said message;

a variable criteria;

information sent to a server and classification data received based on said information;

classification data received from a server; and

stored classification data.

179. A system for combating spam comprising:

a message classifier, operative to provide a spam classification for a message at least partially by relating to a match among network references in said message; and

a message handler, operative to handle said message based on said spam classification.

180. A system for combating spam according to claim 179 and wherein said network references include at least one translatable network address and wherein said match is between at least one translatable network address and another at least one of said network references.

181. A system for combating spam according to claim 180 and wherein said at least one translatable network address comprises a registered network address.

182. A system for combating spam according to claim 180 and wherein said at least one translatable network address comprises an Internet domain name.

183. A system for combating spam according to any of claims 180 – 182 and also comprising an address translator, operative to translate said translatable network address, thereby providing a translated network address.

184. A system for combating spam according to any of claims 179 – 183 and wherein said message handler is operative to perform at least one of the following:

forward said message to an addressee of said message;

store said message in a predefined storage area;

delete said message;

reject said message;

send said message to an originator of said message; and

delay said message for a period of time and thereafter re-classify said message.

185. A system for combating spam according to any of claims 179 – 184 and wherein said message comprises at least one of:

an e-mail;

a network packet;

a digital telecom message; and

an instant messaging message.

186. A system for combating spam according to any of claims 179 – 185 and wherein said message classifier is operative to provide said spam classification at least partially based on at least one of the following:

feedback requested from an addressee of said message;

compliance of said message with a predefined policy;

a registration status of at least one registered address in said message;

a match among network references in said message;

a match between at least one translatable address in said message and at least one other network reference in said message;

at least partial actuation an unsubscribe feature in said message;

an analysis of an unsubscribe feature in said message;

a variable criteria;

information sent to a server and classification data received based on said information;

classification data received from a server; and

stored classification data.